Research Paper | Education | E-ISSN No : 2454-9916 | Volume : 10 | Issue : 3 | March 2024

ETHEREUM ORIENTED ENHANCED SECURE LOG FILE STORAGE USING INTERPLANETARY FILE SYSTEM WITH BLOWFISH ENCRYPTION

Dr. M. S. Anbarasi[1], Barath P.[2], Bharath Y.[3], Arun Kumar J.[4], Ajay A.[5]

[1, 2, 3, 4, 5] Puducherry Technological University, Puducherry

ABSTRACT

In the realm of cloud server operations, where the sheer volume of daily transactions is immense, safeguarding data security is paramount. One of the significant challenges faced is the verification of transaction logs, as attackers may attempt to tamper with them. The current system, utilizing Proof of Work (PoW) for blockchain, falls short by lacking robust data encryption, thereby exposing a critical vulnerability. This proposed paper introduces an innovative solution by integrating the more secure and energy-efficient Proof of Stake (PoS) algorithm with Blowfish encryption. The combination of PoS and Blowfish addresses the identified weaknesses effectively. PoS introduces a novel approach by relying on validators who have a stake in the network, creating a powerful deterrent against log tampering. This not only enhances the integrity of the transaction logs but also reduces the risk of malicious activities. Additionally, the incorporation of Blowfish encryption ensures the confidentiality of log data, providing an extra layer of protection. Even if logs are accessed illicitly, the encryption prevents unauthorized individuals from deciphering sensitive information. Furthermore, the implementation of a smart contract for user registration adds another dimension to security, creating a comprehensive solution to fortify data security on Cloud servers. The proposed approach offers a promising solution to the critical cybersecurity challenge faced by cloud servers. By combining the security features of PoS and Blowfish encryption, along with the strategic use of smart contracts, the solution not only deters tampering but also safeguards sensitive information. This holistic approach contributes significantly to reinforcing the data security infrastructure of cloud servers in the face of evolving cyber threats.

KEYWORDS: Blockchain, Tamper-Resistant, Decentralization, Data Integrity, Blowfish Encryption, Proof of Stake, Smart Contracts

INTRODUCTION

Blockchain

Blockchain technology is a decentralized and transparent system that underpins cryptocurrencies like Bitcoin. It consists of a chain of blocks, each containing a list of transactions, secured through cryptographic hashing. This technology operates without a central authority, relying on consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions and maintain the integrity of the ledger. Smart contracts, self-executing code, enable automated and trustless agreements. The blockchain's immutability and transparency make it suitable for applications beyond finance, such as supply chain management, voting systems, and decentralized applications (DApps). Its potential to revolutionize various industries hinges on addressing scalability and regulatory challenges.

Decentralization

Blockchain operates on a peer-to-peer network of nodes (computers) that work collectively. No single entity, like a central authority or intermediary, has control over the entire network. This decentralization enhances security and transparency.

Blocks

Transactions are grouped into blocks, and each block contains a list of these transactions. Once a block is filled, it's cryptographically sealed, and a new block is created.

Cryptography

Blockchain uses cryptographic techniques to secure data. Each block contains a unique code called a cryptographic hash, which is derived from the data in the block. Changing any data in a block would require changing all subsequent blocks, which is computationally infeasible.

Consensus Mechanisms

To validate and agree on the state of the blockchain, consensus mechanisms are used. The most common one is Proof of Work (PoW), where miners compete to solve complex mathematical puzzles to add a new block. Another method is Proof of Stake (PoS), where validators are chosen to create new blocks based on the amount of cryptocurrency they hold.

MATERIALS AND METHODS

In this section, we use these 4 technologies to implement our project

A. Proof of Stake (POS)

Staking Amount: The quantity of cryptocurrency a participant must hold to become a validator. This parameter determines the level of influence and responsibility a participant has in the PoS consensus mechanism.

Block Time: The interval at which new blocks are created in the blockchain. A shorter block time can enhance the speed of transactions but may require more computational resources.

B. Blowfish Encryption

Key Size: The length of the cryptographic key used for encryption and decryption. Blowfish supports variable key sizes, and the choice of key size influences the algorithm's strength. Common key sizes include 128, 192, and 256 bits.
Block Size: The size of data blocks processed by the encryption algorithm. Blowfish operates on fixed-size blocks, typically 64 bits.

C. Smart Contract

Gas consumption: To evaluate the gas usage of contract functions to optimize for efficiency and cost-effectiveness.

Truffle Tests: An automated testing framework that simplifies the process of testing contracts.

D. IPFS:

IPFS (InterPlanetary File System) is a decentralized protocol and network for storing and sharing content on the internet. It uses unique content addressing, decentralized distribution, and caching to enable efficient and secure retrieval of files without relying on centralized servers. This technology is often used in conjunction with blockchain for creating decentralized applications and services.

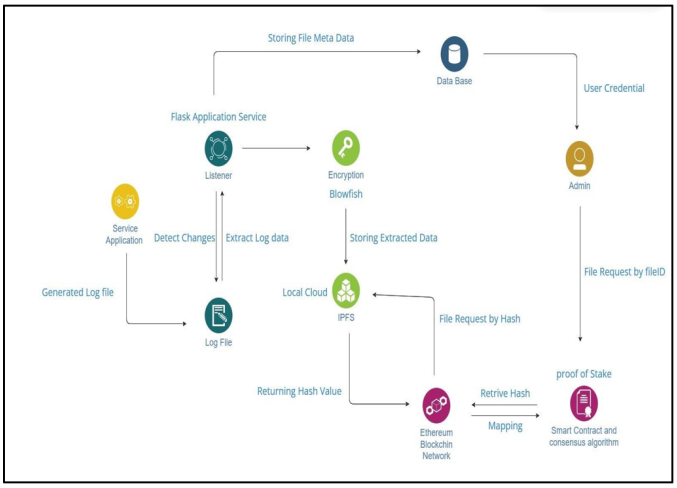

Figure 1. Blockchain And Blowfish encryption for secure log file storage in IPFS

Dataset Used

a. Log Data

Description: Log data represents the information generated by various sources, such as applications, servers, sensors, or devices. It can be in the form of text, JSON, XML, or any other structured or unstructured data.

Attributes:

Log entry ID: A unique identifier for each log entry.
Log message: The content of the log entry.
Log source: Identifies the system or application that generated the log.
Log type: Categorizes the log entry (e.g., error, warning, information).
Timestamp: Records when the event occurred.

b. Timestamps:

Description: Timestamps are essential for establishing the chronological order of log entries. They ensure that events are correctly sequenced in the log file.

Attributes:

Date and time: Precisely when the event occurred.
Timezone information: To ensure consistency in timestamps.

c. Hashes:

Description: Hashes are cryptographic representations of the log data or log entries.

These are used to verify data integrity and detect any tampering.

Attributes:

Hash algorithm: The cryptographic algorithm used (e.g., SHA-256).
Hash value: The result of applying the algorithm to the log data.

d. Transaction Information :

Description: Transaction details related to the blockchain ledger, which stores log entries in a tamper-proof manner.

Attributes:

Transaction ID: A unique identifier for each blockchain transaction.
Sender's address: The originating address for the log entry.
Receiver's address: The recipient's address (e.g., a blockchain smart contract).
Gas cost: The cost associated with the transaction (for Ethereum or similar blockchains).

RESULTS AND DISCUSSION

Justification For The Algorithm Used

Why Blowfish?

The selection of the Blowfish encryption algorithm and the Proof of Stake (PoS) consensus mechanism in our proposed system is driven by their complementary strengths in bolstering the security of cloud servers, particularly in managing transaction logs. Blowfish encryption is chosen for its robustness in providing privacy and integrity to sensitive data. Its symmetric key structure ensures that information is encrypted and decrypted securely, making it an ideal choice for safeguarding transaction logs against unauthorized access or tampering. Its encryption and decryption algorithms are relatively fast. The efficiency of Blowfish, coupled with its well-established track record, contributes to a strong defense against evolving threats.

Why Proof Of Stake?

On the other hand, the incorporation of the Proof of Stake algorithm enhances the overall security posture of the system. PoS eliminates the energy-intensive mining processes associated with Proof of Work, making it environmentally

friendly and economically sustainable. More importantly, PoS introduces a decentralized consensus mechanism where the validation of transactions is based on the stake or ownership of cryptocurrency held by network participants. This ensures that those with a genuine interest in the stability and security of the system are entrusted with validation responsibilities.

CONCLUSION

In conclusion it underscores the critical challenges associated with log file storage within blockchain systems. These challenges are primarily rooted in the existing system's reliance on Proof of Work (PoW) and the absence of data encryption, leaving the log data vulnerable to a host of security threats, including unauthorized access, data breaches, and the potential for data manipulation. Addressing these issues is paramount for the secure and reliable operation of blockchain networks. The proposed work offers an innovative solution that combines the security and efficiency of the Proof of Stake (PoS) consensus algorithm with the robust encryption provided by Blowfish. This approach not only reduces energy consumption and enhances security through validator stakes but also ensures data confidentiality, even when logs are illicitly accessed. The introduction of a smart contract for user registration further bolsters the security framework, discouraging tampering and safeguarding sensitive log data. This comprehensive strategy holds significant promise for bolstering log file storage security in blockchain systems, effectively countering vulnerabilities inherent in the existing system. By mitigating the risks associated with log file breaches and tampering, this proposed approach upholds the integrity of the transaction history, fostering trust in blockchain technology while adhering to the growing global emphasis on sustainability and energy efficiency within the blockchain space.

REFERENCES

1. Parin Patel , Hiren Patel."A Secure Log Storage Mechanism using IPFS and Blockchain Technology". International Journal on Recent and Innovation Trends in Computing and Communication. May 17, 2023 DOI: https://doi.org/10.17762/ijritcc.v11i5s.6592
2. Desheng Yang, Nian Duan, Yang Guo and LuZhang." Medusa: Blockchain Powered LogStorage System". IEEE .Feburary 2020 DOI:10.1109/ICSESS.2018.8663935
3. Louis Shekhtman and Erez Waisbard. "EngraveChain: A Blockchain-Based Tamper-Proof Distributed Log System". Future Internet. 29 May 2021. DOI:10.3390/fi13060143
4. William Pourmajidi, Andriy Miranskyy. " Logchain: Blockchain-assisted Log Storage".IEEE, MAY 22, 2018. DOI:10.1109/CLOUD.2018.00150/
5. Gang Xu , Fan Yun , Yiying Yu , Shiyuan Xu. "A blockchain-based log storage model with efficient query" Springer Nature. June 2nd, 2022. https://doi.org/10.3390/fi13060143
6. Yassine Azizi, Mostafa Azizi, Mohammed Elboukari "Log Data Integrity Solution based on Blockchain Technology and IPFS" , International Journal of Interactive Mobile Technologies (IJIM) ,17 August 2022 , DOI: https://doi.org/10.3991/ijim.v16i15.31713.
7. M. Sato and T. Yamauchi, "Vmm-based log-tampering and loss detection scheme," Journal of Internet Technology, vol. 13, no. 4, pp. 655–666,2012.
8. R. T. Snodgrass, S. S. Yao, and C. Collberg, "Tamper detection in audit logs," in Proceedings of the Thirtieth international conference on Very large data bases-Volume 30.
9. Holt JE. Logcrypt: forward security and public verification for secure audit logs. Proceedings of the 4th Australasian workshops on grid computing and e¬research (ACSW '06), Tasmania, Australia, 2006; 203–211.
10. I. Ray, K. Belyaev, M. Strizhov, D. Mulamba and M. Rajaram, "SecureLogging as a Service—Delegating Log Management to the Cloud,"in IEEE Systems Journal, vol. 7, no. 2, pp. 323-334, June 2013.
11. Omar, Abdullah & Bhuiyan, Md & Basu, Anirban & Kiyomoto, Shinsaku & Rahman, Shahriar(2019). A privacyfriendly platform for healthcare data in Cloud based on Blockchain environment. Future Generation Computer Systems. 95C. 511-521.
12. Dr. Manish Kumar, Ashish Kumar Singh, Dr. T V Suresh Kumar,(2018)Secure Log Storage Using Blockchain and Cloud Infrastructure ,9th ICCCNT 2018, IISC, Bengaluru, India,IEEE'.